IN THE CLAIMS:

Please amend the claims as shown below.

1. (Amended) A process for protecting a computer from hostile code, the process comprising:

defining at least two trust groups, each of the defined trust groups being characterized by a trust group value;

assigning objects and processes in the computer to one of said trust groups, irrespective of the rights of a user of said computer;

defining at least two object types;

assigning an object type to each of the objects;

defining an action rule for each combination of process trust group value, object trust group value, and object type; and,

upon [operation of] an access request by a requesting process [over an] to a target object, performing the action indicated by the action rule applicable to the [comparing a] trust group value of the requesting process, [with a] the trust group value of the target object, and the object type [;

allowing the operation if the trust group value of the process is not smaller than the trust group value of the object; and

disallowing the operation if the trust group value of the process is smaller than the trust group value of the object].

2. (Amended) The process of claim 1 wherein a process is assigned upon creation to the trust group assigned to the passive code from which the process is created.

3. (Amended) The process of claim 1 further comprising changing the trust group of the process if the trust group value of the process is greater than the trust group value of the object.

4. (Amended) The process of claim 1 further comprising changing the trust group of said object [or of said second process] after performing said action [operation].

5. (Amended) The process of claim 1 further comprising, upon creation of an object by a process, assigning said created object to the trust group of said process.

6. (Amended) The process of claim 1 further comprising defining at least two operation types and wherein said combination includes at least one of said operation types [, when said operation is allowed, assigning said process to the trust group of said object or of said second process].

7. (Amended) The process of claim 1 wherein said trust groups are hierarchically ordered, and wherein said process [allowing] further comprises:

allowing said [operation] access request when the trust group of said process is higher or equal in said hierarchy than the trust group of said object [or of said second process; and

denying said operation when the trust group of said process is lower in said hierarchy than the trust group of said object or of said second process].

8. (Amended) The process of claim 7 further comprising assigning said process to the trust group of said object if the trust group of said process is higher than the trust group of said object [or of said second process after the operation is allowed].

9. (Amended) The process of claim [1 further comprising:

defining at least two types of objects;

assigning objects to one of said types; and

wherein the step of allowing operation over an object is further carried out according to the type of said object] 7, wherein upon a restart of said process, the trust group of said process reverts to the original trust group of the object from which the process was created.

10. (Amended) The process of claim 1 further comprising:

defining at least two process types [of processes];

assigning processes to one of said process types[,]; and

wherein said combination includes at least one of said process types [the step of allowing operation of a process is further carried out according to the type of said process].

11. (Amended) The process of claim 1, wherein said object types comprise passive code and executable code [further comprising:

defining at least two types of operations; and

wherein the step of allowing operation of a process over an object or over a second process is further carried out according to the type of said operation].

12. (Amended) The process of claim 6, wherein said operation types comprise open, read, create, modify, and delete [1, further comprising:

defining at least two types of storage methods,

assigning a trust group to a type of storage methods; and

carrying out a storage operation for a process of a trust group according to the storage method assigned to the trust group of said process].

13. (Amended) A computer-readable medium comprising computer readable instructions for protecting a computer from hostile code, the instructions causing the computer to:

define a plurality of trust group values;

define a first and a second rule sets, each of said rule sets comprising a plurality of rules defining an action based on an operation type;

identify objects and processes within the computer;

define a table of at least two trust groups, wherein each trust group comprise one trust group value and said first and second rule sets; and

assign objects and processes in the computer to one of said trust groups irrespective of the rights of a user of said computer;

whereby upon operation of a process over an object, the computer is configured to:

compare a trust group value of the process with a trust group value of the object;

determine whether to allow the operation by following the rules of said first rule set if the trust group value of the process is not smaller than the trust group of the object [;] and

[disallow the operation] following the rules of said second rule set if the trust group value of the process is smaller than the trust group value of the object.

14. (Amended) The computer-readable medium of claim 13 further comprising instructions causing the computer to:

define a table of types of at least two types of objects, the objects in the computer being assigned one type; and

wherein said plurality of rules define said actions further based on the type of said object [the computer accesses said table for allowing said operation].

15. (Amended) The computer-readable medium of claim 13, wherein said operation type comprises open, read, create, modify, and delete [table of trust groups is stored in a non-volatile memory].

16. (Amended) The computer-readable medium of claim 14, wherein said types of objects comprise passive code and executable code [table of types is stored in a non-volatile memory].

17. (Canceled) The computer-readable medium of claim 13, further comprising instructions causing the computer to define a table of rules, and wherein said computer accesses said table of rules.

18. (Canceled) The computer-readable medium of claim 17, wherein said table of rules is stored in a non-volatile memory.

19. (Amended) The computer-readable medium of claim 13, wherein the computer is operatively coupled to a network, the network including a server, the table of trust groups stored in said server.

20. (Canceled) A computer-readable medium according to claim 14, wherein the computer is operatively coupled to a network, the network including a server, the table of types is stored in said server.

21. (Amended) A computer-readable medium according to claim 17, wherein the computer is operatively coupled to a network, the network including a server, the table of rules is stored in said server.

22. (Canceled) A computer-readable medium containing a computer readable instructions for protecting a computer from hostile code, the instructions causing the computer to:

define at least two trust groups, each of the defined trust groups being characterized by a trust group value;

assign objects and processes in the computer to one of said trust groups, irrespective of the rights of a user of said computer;

upon operation of a process over an object, compare a trust group value of the process with a trust group value of the object;

allow the operation if the trust group value of the process is not smaller than the trust group of the object; and

disallow the operation if the trust group value of the process is smaller than the trust group value of the object.

23. (New) A computer comprising:

a read only memory (RAM);

a non-volatile memory;

a processor coupled to said RAM and said non-volatile memory;

wherein said non-volatile memory comprises:

a list of object types;

a list of rules each of said rules defining an action based on an object type;

a list of object trust groups, each trust group defining an object trust value and coupled to at least one of said rules;

a plurality of objects, each of said objects having an object type and assigned to one of said trust groups;

and wherein when a process is created in said RAM from an originating object of one of said objects, said processor assigns to said process a process trust value equal to the object trust value of said originating object.

24. (New) The computer of claim 23, further comprising a controller receiving operation requests from said process to be performed on a target object of one of said objects and, upon receiving said requests said controller access said list of object trust groups, list of rules, and list of object type to determine whether to allow the operation.

25. (New) The computer of claim 24, wherein when the process trust value is not lower than the target object trust value, said controller allows said operation request.

26. (New) The computer of claim 24, wherein when the controller allows the operation request but the process trust value is lower than the target object trust value, said processor resets the process trust value equal to that of the target object trust value.